ISSN:0975-9646

Security in Multi-Cloud Storage with Cooperative Provable Data Possession

Ms. Megha Patil[1], Prof. G.R.Rao[2]

[1, 2] Computer Engineering Department,
BVDUCOE Pune-43(India)

***Abstract*-Data integrity verification is one of the biggest security issue when storage of the data in necessary over cloud. Different methods are available for checking the integrity of data where Provable data possession is one of them. In this paper, we have concentrated on the creation of an efficient PDP method for distributed cloud storage, in which we consider the existence of multiple cloud service providers maintaining and storing client's data in cooperative manner. This cooperatively working PDP method is based on indexing hierarchy method. We show the security of our scheme based on trusted third party and zero-awareness proof structure, which can fulfill reliability of awareness, completeness, and properties. Also, it has used cryptographic algorithm for the security of data while storing over cloud. This technique shows that our solution introduces communication and lower computation overheads in comparison with non-cooperative approaches.**

***Keywords*—Multiple Cloud, Cooperative Provable Data Possession, Homomorphic Variable Reply, Zero awareness, Cloud Storage Security.**

I. INTRODUCTION

Storage of data on cloud is one of the well-known services offered by *cloud computing*. Therefore, subscribers do not need to store their own data on local servers, where in its place their data can be stored on the cloud service provider's storage. Cloud storage gives the facility for users to distantly store their data and enjoy the on-demand high quality cloud applications without the any burden of local hardware and software management, which boasts an array of advantages like capability of storing unlimited data and ability to access data anywhere[1]. Cloud computing has the ability to integrate multiple cloud services together to provide high interoperability environment as it is established based on open architectures and interfaces. Such distributed cloud environment is known as *multi-Cloud*. It uses the adage of not putting all your eggs in one basket. In multi-cloud environment, an enterprise uses two or more clouds, which reduces risk of widely spread loss of data or outage due to a component failure in a single cloud computing environment.

In multi-cloud environment clients can easily access resources remotely by using different interfaces. Web services by using virtual infrastructure management [2] is example it. Various tools and technologies are available in market for multiple clouds such as VMware, vSphere, and Platform VM Orchestrator. For management of client's data, these tools help cloud providers for creating a platform for distributed data storage. But, if such an important platform is susceptible to security attacks, these attacks may introduce irrevocable losses to the clients. For example, the secret information of an enterprise may be illegally accessed by using interfaces, or organization related information and archives may be lost or tampered with when they are stored into an uncertain storage pool outside the enterprise.

One of the biggest issues with cloud data storage is that of data integrity verification at untrusted servers. Also, there exist various motivations like maintaining reputation for cloud service providers (CSP) to behave unfaithfully towards the cloud users. For example, the cloud service provider (CSP), which sometimes suffers Byzantine failures. Such CSP's decide to hide the data errors from the clients for the benefit of their own like for maintaining their reputation or for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Therefore, Security of the data stored over cloud is absolutely necessary for cloud service providers

Different techniques like Provable data possessions [3] (or proofs of retrievability [4]) are important for a storage provider to prove the integrity and ownership of clients' data without any need of downloading it. This property of checking proof without downloading makes it advantage for large-size files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without any need of downloading latest version of data. This leads to replace traditional hash and signature functions in data storage outsourcing. Some recently proposed schemes like Scalable PDP [5] and Dynamic PDP [6][7] mainly focus on PDP issues at untrusted servers in a *single* cloud storage provider. So they are not suitable for a multi-cloud environment.

II. Verification Framework Overview

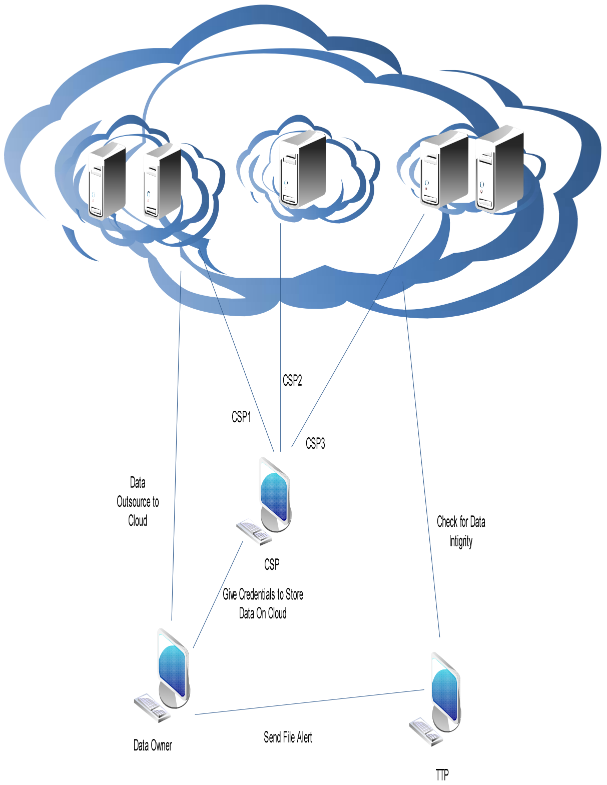


Fig. 1 System Architecture

System architecture shown above involves three different entities: Cooperatively working Cloud Service Providers (CSPs) to provide data storage services have enough storage and computation resources, User of multi-cloud who has a large amount of data to be stored over multiple clouds and have the permissions to access and work on that data gives their data to these cloud service providers[]. Trusted Third Party (TTP) entity is used in this architecture, where this entity offer public query facilities and trusted to store verification parameters for checking integrity of data.

Architecture shown Fig.1 has considered the existence of multiple CSPs working cooperatively to store and maintain the data which is outsourced by client. In order to confirm the reliability of data and to check whether data outsourced over cloud is available or not, this cooperative PDP method is used in all CSPs. As owner of data cannot completely belief to the CSP so here we will use trusted third party for security of outsourced data. Back up servers are also used in this structure for data backup purpose.

III. Coopertive Provable Data Possession Shceme

This work addresses the construction of an efficient method of PDP scheme for distributed cloud storage environment, in which we consider the existence of multiple cloud service providers working cooperatively to store and maintain the clients' data. It shows a *cooperative provable data possession* scheme based on indexing hierarchy. Zero awareness proof system is used to prove the security of this scheme, which can fulfill knowledge reliability and zero-awareness properties.

A. *Indexing hierarchy:*

As data storage is over multiple clouds by converting it into multiple data blocks, indexing method is used for referring to these blocks distributed in multiple clouds.

This arrangement is shown in Figure 2. It has a hierarchy structure resembles representation of file storage. This arrangement consists of three levels as shown in figure which shows relationships among all blocks for stored resources. This structure and different levels are described as follows:

1) Storage Level: This level represents actual storage of data on many physical storage devices.

2) Service Level: This is used for managing multiple services related to cloud storage.

3) Express Level: This level offers an abstract representation of the data blocks or services stored over multiple clouds.

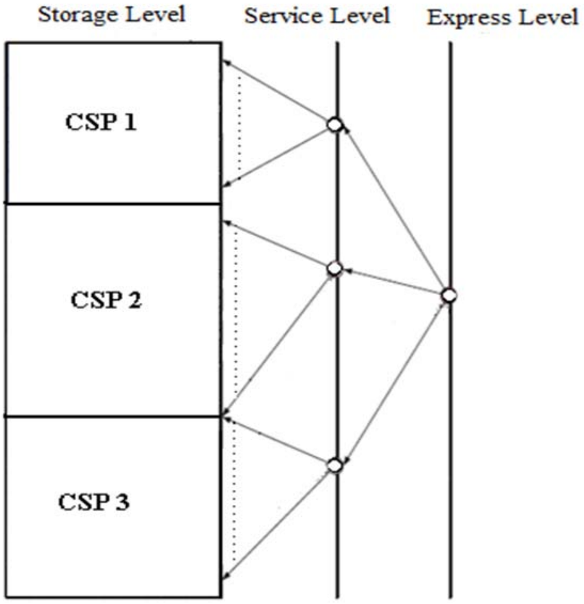


Fig.2 Hash index hierarchy.

This hierarchy used to arrange data blocks from multiple CSP services into a large size file. Above figure shows that the resource in Express Layer are split and stored into three CSPs that are indicated by different colors are shown in Service Layer. After that each CSP fragments and stores the assigned data into the storage servers in Storage Layer. It also makes use of colors to distinguish different CSPs. Moreover, it follows the logical order of the data blocks to organize the Storage Layer.

B. *Homomorphic Verifiable Reply:*

If given two responses θi and θj for two testsQi and Qj from two CSPs, there exist an efficient algorithm to combine them into a response θ corresponding to the sum of the challenges $Qi \cup Qj$ then a response is called homomorphic verifiable reply in a PDP protocol. So, Homomorphic Verifiable Replies is used to combine multiple responses from the different CSPs into a single response.

C. Security Analysis:

For security purpose, cooperative scheme satisfies following properties:

1) Collision resistant indexing: The indexing hierarchy in CPDP scheme is collision resistant. If the client generates files with the same file name and tries to store in multi-cloud, collision because of name doesn't occur there.

2) Public verification property: This Public verification property allows client as well as anyone other than client (data owner) to challenge the cloud server for data integrity and data ownership without the need for any secret information.

3) Zero-awareness property: Privacy of the data blocks stored in multi-cloud and signature tags can be preserved by using this verification property.

4) Knowledge reliability verification: It is not possible to fool the verifier easily to accept false statements. These structures can also oppose the tag forgery attacks, which help to avoid cheating the CSPs' owner. This property is responsible for avoiding tampering of the data or tag forgery, when collisions tried.

IV. Module Information

Module1. Login and Registration

In this we will develop the Login and Registration GUI for Entities included in Project.

Module2. Cloud Customer

The Customer or User of the Cloud is one who has a large amount of data to be stored in multiple clouds and have the permissions to use and access stored data. Before uploading process, User's Data is converted into data blocks. That data blocks are uploaded over multiple clouds in uploading process. The TTP outlooks the data blocks Uploaded in multi cloud. The user can also update the data uploaded over multiple clouds. If the client wishes to download their files, the data from multi cloud is integrated sequentially and downloaded.

Module3. Trusted Third Party

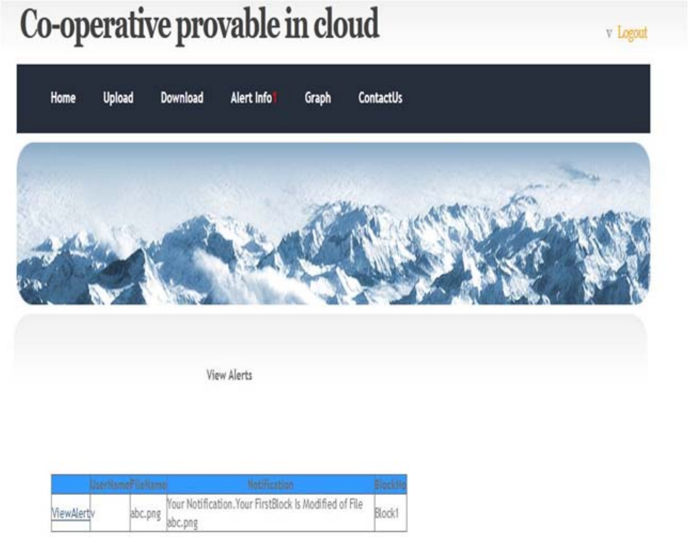
Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In this system the Trusted Third Party, outlook the user data blocks and uploaded to the distributed cloud. In distributed environment of cloud each cloud has user data blocks. If anybody tries to change the data stored over cloud Trusted Third Party gets alert of it that is again sent to client.

Module4. Multi cloud storage

In this system the each cloud admin will be having data blocks stored over their cloud. Cloud computing has the ability to integrate multiple cloud services together to provide high interoperability environment as it is established based on open architectures and interfaces. Such distributed cloud environment where multiple clouds are working cooperatively is known as *multi-Cloud*. In this section, user uploads the data into multi cloud.

V Screenshot

In this section we present, screenshot for Alert Generation. If any Modification is done in files uploaded



	UserName	FileName	Notification	BlockNo
ViewAlert	v	abc.png	Your Notification.Your FirstBlock Is Modified of File abc.png	Block1

Fig.3 Alert generation

Conclusion And Future Work

From research, we have presented an efficient method for security of data outsourced over multi-cloud. This research, efficient method of PDP scheme is constructed for distributed cloud storage. This scheme provided all security properties required by zero knowledge interactive proof system. . Based on indexing, we have planned a cooperative scheme to support dynamic scalability using multiple storage servers.

There are multiple cloud service providers for multiple clouds as we are using multiple clouds. Central Cloud Service Provider is used for minimizing the complexity as we want to store data block in each cloud, the request has to go from each Cloud Service Provider. Thus, Cloud Service Providers manages requests. During uploading and downloading User has to answer the Security Question. Security Questions and Answers are submitted by user during the registration phase. So during Uploading/Downloading operation If user is normal then he can answer that security questions if he/she is intruder then he/she cannot answer that questions. Thus, using this we can provide more Security. Also, we can use encryption algorithm [9] for provide the Security to uploaded data and the digest

References

[1] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage" *IEEE*, Mengyang Yu, Dec-2012

[2] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, "Virtual infrastructure management in private and hybrid Clouds," *IEEE Internet Computing*, vol. 13, no. 5, pp. 14–22, 2009.

[3] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in *ACM Conference on Computer and Communications Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[4] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for Large files," in *ACM Conference on Computer and Communications Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th international conference on Security and privacy in Communication networks*, *Secure Comm*, 2008, pp. 1–10.

[6] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced Storages in clouds," in *SAC*, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[7] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *ACM Conference on Computer and Communications Security*, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[8] L. Fortnow, J. Rompel, and M. Sipser, "On the power of multiprover Interactive protocols," in *Theoretical Computer Science*, 1988, pp. 156–161.

[9] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'2001)*, vol. 2139 of LNCS, 2001, pp. 213–229.